

Notice of Allowability

Application No.

09/482,928

Examiner

CUONG H. NGUYEN

Applicant(s)

BLINN ET AL.

Art Unit

3661

– The MAILING DATE of this communication appears on the cover sheet with the correspondence address–

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 5/25/04.
2. ☒ The allowed claim(s) is/are 130-133; they are renumbered as claims 1-4.
3. ☒ The drawings filed on 13 January 2000 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
 - * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

CUONG H. NGUYEN
Primary Examiner
Art Unit: 3661

S.N. 09/482,928
Art Unit 3661

DETAILED ACTION

1. This Office Action is the answer to the election filed on 5/25/2004 wherein pending claims 130-133 are elected, and pending claims 106-129, 134-157 have been canceled.
2. Claims 130-133 are pending in this application.

Allowable subject matter

3. Independent claim 130 is patentable distinct over closest cited documents of Cuccia et al., and Downs et al. because said prior art do not disclose a method for a device to interdependently validate a piece of digital content and a corresponding digital license for rendering the digital content, the digital content being encrypted, the encrypted digital content being decrypt able according to a decryption key (KD) and being packaged in a digital content package, the digital content package being provided by a content provider having a public key (PU-C) and a private key (PR-C), the digital license being provided by a license provider having a public key (PU-L) and a private key (PRL), the device having a public key (PU-D) and a private key (PR-D), the digital content package comprising: the encrypted digital content; and the content provider public key (PU-C) encrypted with the decryption key (KD) and signed by the content provider private key (PR-C) (i.e., (KD (PU-C) S (PR-

S.N. 09/482,928
Art Unit 3661

C)); the digital license comprising: the decryption key (KD) encrypted with the device public key (PU-D) (i.e., (PU-D (KD))); a digital signature from the license provider (without any attached certificate) based on (KD (DR-L)) and (PU-D (KD)) and encrypted with the license provider private key (i. e., (S (PR-L))); and a certificate containing the license provider public key (PU-L) and signed by the content provider private key (PR-C) (i.e., (CERT (PU-L) S (PR-C))); the method comprising:

- obtaining (PU-D (KD)) from the license; applying (PR-D) to (PU-D (KD)) to produce (KD), obtaining (KD (PU-C) S (PR-C)) from the digital content package; applying (KD) to (KD (PU-C) S (PR-C)) to produce (PU-C);
- applying (PU-C) to (S (PR-C)) to validate (KD (PU-C) S (PR-C)), thereby validating the digital content package; obtaining (CERT (PU-L) S (PR-C)) from the license; applying (PU-C) to (CERT (PU-L) S (PR-C)) to validate (CERT (PU-L) S (PR-C)), thereby validating the content provider, and also to obtain (PU-L);

obtaining (S (PR-L)) from the license; and applying (PU-L) to (S (PR-L)), thereby validating the license.

4. Claims 131-133 are allowed because they are dependent on their parent claim 130.

Conclusion

5. Claims **130-133** are allowed. They are renumbered as claims 1-4 (in that order).

6. These references are considered pertinent to applicants' disclosure; however, they do not disclose that a content provider's public key is encrypted with a decryption key, and signed by the content provider private key:

- **Cuccia et al.**, US Pat. 6,151,676 disclose about administration and utilization of secret fresh random numbers in a networked environment, November 21, 2000
- **Yoshiura et al.**, US-PAT-NO: 6131162, disclose about a digital data authentication method, 10/10/2000.
- **Atalla**, US Pat. 5,960,086, discloses unified end-to-end security methods and systems for operating on insecure networks, September 28, 1999.
- **Hasebe et al.**, US Pat. 5,555,304 disclose a storage medium for preventing an illegal use by a third party, September 10, 1996.
- **Krishnan**, (US Pat.6073124 - 6/06/2000), Method and system for securely incorporating electronic information into an online purchasing application.

S.N. 09/482,928
Art Unit 3661

- **Stefik**, (US Pat. 5,715,403), discloses about a system for controlling the distribution and use of digital works having attached usage rights where the usage rights are defined by a usage rights grammar.
- **Stefik et al.**, (US Pat. 5,629,980), discloses about a system for controlling the distribution and use of digital works.
- **Van Wie et al.**, (US Pat. 5,943,422), discloses about a steganographic techniques for securely delivering electronic digital rights management control information over insecure communication channels.
- **Ginter et al.**, (US Pat. 5,982,891), discloses about a system and a method for secure transaction management and electronic rights protection.
- From findarticles.com, SSP solutions awarded key technology patent, uniquely secures biometric identification against falsification, Business Wire, 9/18/2001.
- From findarticles.com, HDCP: what it is and how to use it; whether or not you believe in content protection, if you design digital-video products, you must deal with the technology..., EDN, 4/18/2002.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CUONG H. NGUYEN whose telephone number is 703-305-4553. The examiner can normally be reached on 7am - 3:30pm.

S.N. 09/482,928
Art Unit 3661

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, THOMAS G. BLACK can be reached on 703-305-8233. The fax phone number for the organization where this application is assigned is 703-305-7687. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Cuong Nguyen

CHAN
CUONG H. NGUYEN
Primary Examiner
Art Unit 3661